Doc Code: AP.PRE.REQ

PTO/SB/33 (07/05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
RSW920010086US1	

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
10/043,355	01/09/2002
First Named Inventor	
Jason R. McGee	
Art Unit	**Examiner**
2144	T. Nguyen

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 33,023

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Theodcre Naccarella/
Signature

Theodore Naccarella
Typed or printed name

215-923-4466
Telephone number

June 29, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Tradeamrk Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Jason Robert McGee, Christopher C. Mitchell, Michael John Morton and Brent A. Peters**

Examiner: **Thanh Nguyen**

Group Art: **2144**

Application No.: **10/043,355**

Confirmation No.: **7289**

Filing Date: **January 9, 2002**

Docket No.: **RSW920010086US1**

Title: **METHOD AND APPARATUS FOR SYNCHRONIZING COOKIES ACROSS MULTIPLE CLIENT MACHINES**

FILED ELECTRONICALLY

Commissioner for Patents
Post Office Box 1450
Alexandria, VA 22313-1450

ARGUMENTS FOR PRE-APPEAL BRIEF CONFERENCE

Sir:

All claims stand rejected as obvious over Howard in view of Sears and JSOnline.

The Present Invention: The present invention is a method for synchronizing copies of the same cookie across a plurality of different client computers of a single user. Particularly, a person may have multiple computers that she uses to access the Web. According to the invention, the user registers all her computers with a service that will synchronize the copies of the cookies across all of her computers. A Cookie Synchronization Server (CSS) stores the cookie information. Each of the user's client computers tracks changes made to cookies at that machine and sends any cookie change data to the CSS. The CSS stores the data and later sends it out to each other client machine of that account.

Howard: Howard discloses a technique for simplifying for a computer user the accessing of web sites that require registration (e.g., a user ID and password). Specifically, a plurality of web sites register to be part of this service. The servers operated by those web sites are termed "affiliate servers". In addition, an "authentication server" is maintained. When a user accesses an affiliate web server that requires a user ID and/or password, the affiliate server passes the client request to the authentication server instead of servicing it itself. (Col. 6, ll. 55-57). The authentication server sends the client machine a sign-in page. (Col. 6, ll. 59-62). When the user enters the proper password and ID, the authentication server copies certain cookies to the client machine and redirects the user's browser back to the affiliate server. (Col. 7, ll. 16-20). These cookies comprise a first cookie that indicates the time that the user was authenticated and a second cookie containing the user's profile. (Col. 7, ll. 23-27). These two cookies

cannot be read by any affiliate servers. (Col. 7, ll. 40-41). The authentication server also generates an authentication ticket and transmits it to the affiliate server informing the affiliate server that the user has been properly authenticated. (Col. 7, ll. 47-52). The authentication server also communicates the user profile information to the affiliate server through the client machines. (Col. 7, ll. 58-67). The authentication server also creates and maintains a cookie that contains a list of the affiliate servers visited by the used during a network session and then, when the used logs off the network, sends to each affiliate server on that list, a request for the affiliate server to delete any cookies it placed on the client computer system. (Col. 7, ll. 27-38).

Hence, Howard merely permits a single user to be authenticated on multiple web sites with the same ID and password by entering that ID and password only once per internet session. Howard has nothing to do with maintaining copies of the same cookie across a plurality of different client machines.

Sears: In Sears, a number of web sites register with a server (the "cookie server") and provide it with information regarding what data fields it wants in cookies of users of that web site. These registered sites are listed in a cookie list stored at the cookie server and are provided to the client when the client logs into the cookie server. When a client initiates a connection to a web site within the cookie list, in addition to checking for any locally stored cookies, the client indicates to the cookie server that it is connecting to that web site. The cookie server then uses the cookie requirement information that it obtained from that web site, as well as user specific information, to generate one or more appropriate cookies for that web site and transmits them to the client. The client then uses those cookies in the course of navigating the web site. This allows a user to type in a piece of data once and then access different Web sites without having to re-enter the same information again. The client machine need not store the cookie. The automatically generated cookie for a particular web site may be stored at the cookie server and transmitted to the client only when the client navigates to the web site. For example, a user may have hundreds of cookies for hundreds of different Web sites. If the user changes his home address, instead of entering the same data hundreds of times (i.e., once for each Web site), the user enters it once and transmits it to the cookie server. The cookie server would then update all of the cookies that the server is storing.

Sears does not mention anything about maintaining copies of the same cookie across a plurality of different client machines. Rather, Sears deals with maintaining consistency of information in different cookies in the same machine. Sears discusses only one user client machine.

JSOnline: JSOnline discusses Web bugs, which some Web sites use to secretly gather information about visitors. The Office focuses on a single paragraph in JSOnline that states "Using a web bug process called 'cookie sync,' two companies can exchange data in the background about Web site visitors". The Office asserts that this teaches the feature of synchronizing a cookie across said plurality of

client computing devices containing a different copy of said cookie. Nothing could be further from the truth. There is only one client machine in JSOnline. The quoted paragraph concerns sharing of information between two servers. Furthermore, despite being called "cookie sync", it does not involve synchronizing cookies at all (i.e., causing two copies of a cookie to be identical). The exemplary use of "cookie sync" described in JSOnline is (1) a user surfs to xyz.com, which contains a Web bug that looks like an image embedded in the Web page; (2) in response to loading the Web page, the user's computer fetches the image, which is actually located at Bug.com; (3) the user's client machine contacts Bug.com, which delivers an invisible image. Effectively, xyz.com has tricked the user's client machine into transmitting information from xyz.com and/or the user's client machine to Bug.com without the user's knowledge. Thus, Bug.com can potentially determine the type of browser that fetched the Web bug image, the IP address of the computer that fetched the Web bug, and a previously-set cookie value.

In any event, despite the name, no actual synchronizing of cookies occurs at all, let alone across a plurality of client machines.

The Combination: The proposed combination is not suggested nor would any combination of the three references result in a system that synchronizes the same cookie at different client machines. None of the three applied prior art references even discusses more than one client machine, let alone has anything to do with synchronizing different copies of the same cookie across a plurality of client machines, which is the subject matter of the present claims. Therefore, no combination of the reference could possibly suggest as much.

The Claim Elements of Exemplary Claim 1: Furthermore, in any event, none of these references discloses any of the teachings for which it has been cited. None of the references even pertains to the subject matter of the present invention, namely, synchronizing the same cookie across a plurality of different client machines used by a single user entity.

The Office asserts that the first portion of claim element (1), i.e., registering a plurality of client computing devices as members of an account, is taught in Howard col. 2, ll. 15-42 and col. 5, ll. 42-67 wherein the user of the client machine registers by providing necessary information to the authentication server. These portions of Howard described that "the user of client computer system 100 and the operator of affiliate server 104 'register' with the authentication server 110". (Col. 5, ll. 48-51). This is a discussion of a single client computer, not a plurality of client computers that are members of an "account". Accordingly, this portion of Howard does not disclose "registering a plurality of client computing devices as members of an account".

With respect to the second portion of claim element (1), which recites "wherein at least one cookie is to be synchronized across said plurality of client computing devices that are members of said account, each of said plurality of client computing devices containing a different copy of said at least one

cookie", the Office asserts that this is found in JSOnline which discloses using a web bug process called "cookie sync" so that two companies can exchange data in the background about website visitors. However, as described above, "cookie sync" concerns two servers sharing information that can be obtained from a cookie on the client machine. It has nothing to do with sharing cookies per se, let alone sharing them amongst client machines.

The second paragraph of claim 1 recites "maintaining information identifying the members of said account at a server on said network". The Office asserts that this is found in claim 1 of Howard and comprises the information received in the completed web page authentication information maintained by the authentication server. This is not an accurate description of claim 1 of Howard. The Office is referring to the 5th and 6th paragraphs of claim 1 which recite "communicating a web [page] from the authentication server to an Internet browser operated by the user, wherein the web page requests login information to be returned to the authentication server from the user" and "receiving the completed web page at the authentication server from the user".

First, the authentication information (i.e., ID and password) in the returned web page does not disclose the identity of the client machines that are members of the account. Secondly, there is only one member of the account. Accordingly, Howard does not disclose this claim element.

The third element of claim 1 recites "responsive to a change in a copy of said at least one cookie stored at a first one of said client computing devices that is a member of said account, said first member client computing device sending a message to said server on said network, said message containing sufficient data from which said changes to said copy of said at least one cookie can be determined and the account to which said first member client computing device corresponds".

The Office asserts that this is found in Sears at col. 3, ll. 32-48 and col. 10, l. 51-col. 11, l. 6. These portion of Sears describe the user changing the data in the data field stored at the cookie server and then the cookie server placing that data into one or more different cookies at the cookie server. This differs from the claim element. Specifically, there is no cookie at the client that is being changed and to which the further processing is responsive, as claimed. There are no cookies at the client at all. The whole point of Sears is that the client does not store cookies. Rather, the cookie server stores data that is needed to generate data fields within cookies and, when the client navigates to a web site in the cookie server's cookie list, the cookie server builds the appropriate cookie(s) for that particular web site and sends it to the client.

The fourth element of claim 1 recites "storing said data at said server". The "data" is the data recited in element (3), namely, the cookie changes at the client and the account ID. The Office asserts that this is found in col. 3, l. 59-col. 4, l. 2 of Howard in which the authentication server provides user profile information to the affiliate server.

This portion of Howard discloses the authentication server sending user information to the affiliate server and is irrelevant to this claim element. User profile information is not cookie change data as defined in claim 1.

The fifth element of claim 1 recites "said server sending said data to other client computing devices that are members of said account". The Office asserts that this is found in Howard at col. 7, ll. 34-35. This portion of Howard states "when the user logs out, the authentication server sends a message to each Web server on the list of sites visited. Each message is a request for the Web server to delete any cookies it placed on the client computer system (e.g., through a browser running on the client computer system)". This feature of sending a message from the authentication server to the affiliate server asking the affiliate server to delete cookies when the user logs off is irrelevant to the claimed feature of a server sending changed cookie information to the other clients of the given account. Specifically, (1) a request to delete cookies is not changed cookie information and (2) an affiliate server is not a client.

The sixth element of claim 1 recites "each of said other client computing devices that is a member of said account updating its copy of said at least one cookie in accordance with said data". The Office asserts that this is found in Howard at the same col. 7, ll. 25-39 concerning the authentication server updating the cookie that contains the list of sites visited by the user. Specifically, this portion of Howard discusses the authentication server maintaining a cookie listing the sites visited by the user and sending a message to affiliate servers asking them to delete cookies they placed on the client machine. Neither of these features has anything to do with client machines updating their cookie data. This cookie is not sent to any other computer. It only contains a list of affiliate servers to which a request to delete cookies will be sent. Nothing at all is sent to any client. Even further, deleting a cookie does not comprise updating a copy of a cookie in accordance with changed cookie data as that term is used in the present application.

Thus, the prior art actually does not disclose any element of claim 1, let alone all of them. This result is not surprising since none of the three cited references has anything to do with sharing cookies across multiple client machines.

Respectfully submitted,

June 29, 2007
DATE

/Theodore Naccarella/
Theodore Naccarella, Reg. No. 33,023
Synnestvedt & Lechner LLP
2600 Aramark Tower
1101 Market Street
Philadelphia, PA 19107-2950